Linear independence of rank 1 matrices and the dimension of $*$-products of codes

Hugues Randriambololona
ENST "Telecom ParisTech" & LTCI CNRS UMR 5141

January 27, 2015

Abstract

We show that with high probability, random rank 1 matrices over a finite field are in (linearly) general position, at least provided their shape $k \times l$ is not excessively unbalanced. This translates into saying that the dimension of the $*$-product of two $[n, k]$ and $[n, l]$ random codes is equal to $\min(n, kl)$, as one would have expected. Our work is inspired by a similar result of Cascudo-Cramer-Mirandola-Zémor [4] dealing with $*$-squares of codes, which it complements, especially regarding applications to the analysis of McEliece-type cryptosystems [5][6]. We also briefly mention the case of higher $*$-powers, which require to take the Frobenius into account. We then conclude with some open problems.

1 Introduction

Many fundamental problems in information theory and in theoretical computer science can be expressed in terms of the structure of linearly independent and generating subsets of a set in a vector space, as illustrated by [10] and the subsequent success of matroid theory. In this context the importance of the following definition is self-evident:

Definition 0. *Let V be a finite-dimensional vector space, over an arbitrary field. We say a set $X \subseteq V$ is in general position if any finite subset $S \subseteq X$ has its linear span $\langle S \rangle$ of dimension*

$$\dim\langle S \rangle = \min(|S|, \dim V).$$

This means that there are no more linear relations than expected between elements of X: any $S \subseteq X$ of size $|S| \leq \dim V$ is linearly independent, and any $S \subseteq X$ of size $|S| \geq \dim V$ is a generating set in V.

This requirement is quite strong, and weaker variants have been considered. We can cite at least three of them.

The first one is to introduce thresholds. We say X is in (a, b)-general position if any $S \subseteq X$ of size $|S| \leq a$ is linearly independent, and any $S \subseteq X$ of size

$|S| \geq b$ is a generating set in V. This notion should look very familiar to coding experts. Indeed one shows easily:

Lemma 1. *Let C be a q-ary $[n,k]$ code, with generating matrix G. Set $V = \mathbb{F}_q^k$ and let $X \subseteq V$ be the set of columns of G. Then X is in (a,b)-general position, with $a = \mathrm{d}_{\min}(C^\perp) - 1$ and $b = n - \mathrm{d}_{\min}(C) + 1$.*

A second one is to allow a small gap g from the expected dimension: we say X is in g-almost general position if for any $S \subseteq X$ we have

$$\dim\langle S\rangle \geq \min(|S|, \dim V) - g.$$

This means allowing up to g more linear relations than expected. There is an obvious link with the previous notion:

Lemma 2. *If $X \subseteq V$ is in (a,b)-general position, then it is in g-almost general position for $g = \min(\dim V - a, b - \dim V)$.*

We leave it to the reader to combine Lemma 1 and Lemma 2 and give a coding-theoretic interpretation of this integer g (or a geometric interpretation in case C is an AG-code).

Last, our third variant is probabilistic, allowing a small proportion of S to fail in Definition 0. In fact, rather than subsets of X, it will be easier to consider sequences of elements of X, possibly with repetitions. For this we will assume that X is equipped with a probability distribution $\mathscr{L}$. A natural choice when X is finite would be to take the uniform distribution, however more general $\mathscr{L}$ will be allowed. Then, measuring how close $X \subseteq V$ is to being in general position reduces to the following:

Problem 3. *Let $n \geq 1$, and $\mathbf{u_1}, \ldots, \mathbf{u_n}$ random elements of X (understood: independent, and distributed according to $\mathscr{L}$). Give bounds on the "error probability"*

$$\mathbb{P}[\dim\langle \mathbf{u_1}, \ldots, \mathbf{u_n}\rangle < \min(n, \dim V)].$$

In this work we address this problem for $V = \mathbb{F}_q^{k\times l}$ a matrix space, and $X \subseteq V$ the set of matrices of rank 1.

Understanding the linear span of families of rank 1 matrices is especially important regarding the theory of bilinear complexity (or equivalently, that of tensor decomposition). Indeed, computing the complexity of a bilinear map (or the rank of a 3-tensor) reduces to the following [2][3][7][8]: given a linear subspace $W \subseteq \mathbb{F}_q^{k\times l}$, find a family of rank 1 matrices of minimal cardinality whose linear span contains W.

Another motivation comes from the theory of $*$-products of codes, and in particular its use in a certain class of attacks [5][6] against McEliece-type cryptosystems. Given words $\mathbf{c} = (c_1, \ldots, c_n), \mathbf{c'} = (c'_1, \ldots, c'_n) \in \mathbb{F}_q^n$, we let $\mathbf{c} * \mathbf{c'} = (c_1c'_1, \ldots, c_nc'_n) \in \mathbb{F}_q^n$ be their componentwise product. Then [9] if $C, C' \subseteq \mathbb{F}_q^n$ are two linear codes of the same length, their product $C * C' \subseteq \mathbb{F}_q^n$ is defined as the linear span of the $\mathbf{c} * \mathbf{c'}$ for $\mathbf{c} \in C, \mathbf{c'} \in C'$. We can also define the square $C^{\langle 2\rangle} = C * C$, and likewise for higher powers $C^{\langle j\rangle}$.

Setting $k = \dim C$ and $l = \dim C'$, it is then easily seen

$$\dim C * C' \leq kl,$$

$$\dim C^{\langle 2 \rangle} \leq k(k+1)/2,$$

and in fact for small k, l and random C, C' one expects these inequalities to be equalities. For the second inequality, this is proved in [4]. For the first inequality, we will see this reduces to our solution of Problem 3 for rank 1 matrices.

So, together, [4] and our results support the heuristic at the heart of the aforementionned attacks against McEliece-type cryptosystems. Indeed, the very principle of these attacks is to uncover the hidden algebraic structure of an apparently random code (which serves as the public key) by identifying subcodes for which equality fails in these inequalities (for instance, the dimension of the product behaving additively rather than multiplicatively).

2 Generic approach

Here V is an abstract vector space of dimension m over $\mathbb{F}_q$, and $X \subseteq V$ an arbitrary subset. We may assume X spans V. We are interested in the function

$$\mathbb{P}(n) = \mathbb{P}[\dim\langle \mathbf{u_1}, \ldots, \mathbf{u_n} \rangle < \min(n, \dim V)].$$

Clearly it is unimodal, more precisely it is increasing for $n \leq m$ and decreasing for $n \geq m$. Now we study each of these two cases in more detail.

2.1 Case $n \geq m$.

We have $\dim\langle \mathbf{u_1}, \ldots, \mathbf{u_n} \rangle < m$ iff $\mathbf{u_1}, \ldots, \mathbf{u_n}$ are contained in an hyperplane H of V. Using the union bound and the independence of the $\mathbf{u_i}$ we get at once:

Proposition 4. *We have*

$$\begin{aligned} \mathbb{P}(n) &\leq \sum_H \mathbb{P}[\mathbf{u_1}, \ldots, \mathbf{u_n} \in H] \\ &= \sum_H \mathbb{P}[\mathbf{u_1} \in H]^n \end{aligned}$$

where H ranges over hyperplanes of V.

This bound is exponentially small. More precisely, set

$$\rho = \max_H \mathbb{P}[\mathbf{u_1} \in H]$$

(for instance $\rho = \max_H |X \cap H|/|X|$ if $\mathscr{L}$ is uniform distribution). We then see immediately:

Corollary 5. *For all $n \geq m$ we have*

$$c\rho^{n-m} \leq \mathbb{P}(n) \leq c'\rho^{n-m}.$$

where $c = \rho^m$ and $c' = \sum_H \mathbb{P}[\mathbf{u_1} \in H]^m$.

It should be noted that c, c', ρ depend on V and X. So, part of the job will be to make these constants more explicit when V and X will be specified.

Another interesting fact is that the RHS in Proposition 4 is

$$\sum_H \mathbb{P}[\mathbf{u_1}, \ldots, \mathbf{u_n} \in H] = \mathbb{E}[|\{H;\ \mathbf{u_1}, \ldots, \mathbf{u_n} \in H\}|],$$

the expected value of the number of hyperplanes containing $\mathbf{u_1}, \ldots, \mathbf{u_n}$. However, this number is precisely $\frac{q^d-1}{q-1}$, where $d = \operatorname{codim}\langle \mathbf{u_1}, \ldots, \mathbf{u_n}\rangle$. This allows us to combine our second and third variants of the notion of general position:

Proposition 6. *For $0 \leq g \leq \min(m, n)$ we have*

$$\mathbb{P}[\dim\langle \mathbf{u_1}, \ldots, \mathbf{u_n}\rangle < m - g] \leq c'\rho^{n-m}\frac{q-1}{q^{g+1}-1}$$

(with c', ρ as above), and also

$$\mathbb{P}[\dim\langle \mathbf{u_1}, \ldots, \mathbf{u_n}\rangle < m - g] \leq \sum_W \mathbb{P}[\mathbf{u_1} \in W]^n$$

where $W \subseteq V$ ranges over subspaces of codimension $g + 1$.

Proof. The first inequality follows from the discussion above, using Markov's inequality as in [4, Prop. 5.1]. The second is a direct approach using the union bound similar to that of Proposition 4. □

Which of these two bounds is stronger, and which is more tractable, certainly depends on V and X. Note also that the bounds remain valid even without the assumption $m \leq n$.

We illustrate what precedes for $X = V = \mathbb{F}_q^m$ with uniform distribution (this will be used later). We introduce the converging infinite product

$$C_q = \prod_{j \geq 1}(1 - q^{-j})^{-1}.$$

Numerically, $C_q \leq C_2 \approx 3.463$.

We let $\begin{bmatrix} m \\ r \end{bmatrix}_q = \prod_{1 \leq j \leq r} \frac{q^{m-r+j}-1}{q^j-1}$ denote the number of r-dimensional subspaces in $\mathbb{F}_q^m$.

Lemma 7. *We have*

$$q^{r(m-r)} \leq \begin{bmatrix} m \\ r \end{bmatrix}_q \leq C_q q^{r(m-r)}.$$

Proof. From $q^{m-r} \leq \frac{q^{m-r+j}-1}{q^j-1} \leq (1-q^{-j})^{-1}q^{m-r}$. □

Proposition 8. *For $0 \leq r \leq \min(m,n)$ and random $\mathbf{u_1}, \dots, \mathbf{u_n} \in \mathbb{F}_q^m$ uniformly distributed, we have*

$$\mathbb{P}[\dim\langle \mathbf{u_1}, \dots, \mathbf{u_n}\rangle \leq r] \leq C_q q^{-(n-r)(m-r)}.$$

Proof. Follows from what precedes, using $\mathbb{P}[\mathbf{u_1} \in W] = q^{-(m-r)}$ for $\dim W = r$. □

2.2 Case $n \leq m$.

From now on we will suppose $(X, \mathscr{L})$ is homothety invariant: given any $\lambda \in \mathbb{F}_q^\times$, then for random $\mathbf{u} \in X$, we also have $\lambda\mathbf{u} \in X$, with the same distribution $\mathscr{L}$.

We say a vector $\mathbf{z} = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_q^n$ is a linear relation for $\mathbf{u_1}, \dots, \mathbf{u_n}$ if $\lambda_1\mathbf{u_1} + \cdots + \lambda_n\mathbf{u_n} = 0$.

Also introduce the random variable

$$\mathbf{s_n} = \mathbf{u_1} + \cdots + \mathbf{u_n} \in V.$$

Lemma 9. *For any $\mathbf{z} \in \mathbb{F}_q^n$ of Hamming weight w, we have*

$$\mathbb{P}[\mathbf{z} \text{ is a linear relation for } \mathbf{u_1}, \dots, \mathbf{u_n}] \;=\; \mathbb{P}[\mathbf{s_w} = 0].$$

Proof. We may suppose $\mathbf{z}$ has support $\{1, \dots, w\}$, and we conclude since $\mathbf{u_i}$ and $\lambda_i\mathbf{u_i}$ have same distribution for $\lambda_i \neq 0$. □

Proposition 10. *We have*

$$\mathbb{P}(n) \leq \sum_{w \geq 1} \binom{n}{w} (q-1)^{w-1} \mathbb{P}[\mathbf{s_w} = 0]$$

Proof. Union bound, as in Proposition 4 (note that we may count linear relations only up to proportionality). □

Likewise, Markov's inequality gives, for any $g \geq 0$,

$$\mathbb{P}(\dim\langle \mathbf{u_1}, \dots, \mathbf{u_n}\rangle < n-g) \leq \tfrac{1}{q^{g+1}-1} \sum_{w \geq 1} \tbinom{n}{w} (q-1)^w \mathbb{P}[\mathbf{s_w} = 0].$$

In these sums we expect the contribution of linear relations of large weight should stay under control thanks to:

Proposition 11. *As $w \to \infty$ we have*

$$\mathbb{P}[\mathbf{s_w} = 0] \to \frac{1}{q^m},$$

except for $q = 2$ and X contained in the translate of an hyperplane, in which case we have $\mathbb{P}[\mathbf{s_w} = 0]$ for odd w, and $\mathbb{P}[\mathbf{s_w} = 0] \to \frac{1}{2^{m-1}}$ for even $w \to \infty$.

Proof. We treat first the case $q > 2$, so there is a $\lambda \neq 0, 1$ in $\mathbb{F}_q$. The $\mathbf{s_w}$ form a random walk on the finite commutative group V. Seen as a Markov chain, it is irreducible, because X spans V (as a vector space, but also as a group, since X is homothety-invariant). Moreover it is aperiodic, because the zero vector can be written as a sum of 2 elements of X (*e.g.* $\mathbf{s} + (-\mathbf{s})$), and also as a sum of 3 elements of X (*e.g.* $(1-\lambda)\mathbf{s} + (-\mathbf{s}) + \lambda\mathbf{s}$). So it converges to its unique stationnary distribution, which can only be uniform.

The case $q = 2$ is similar, with a tweak on aperiodicity. □

3 Rank 1 matrices

A matrix $\mathbf{u} \in \mathbb{F}_q^{k\times l}$ is of rank 1 iff it can be written $\mathbf{u} = \mathbf{p}\mathbf{q}^T$ for column vectors $\mathbf{p} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}$, $\mathbf{q} \in \mathbb{F}_q^l \setminus \{\mathbf{0}\}$. Moreover these $\mathbf{p}, \mathbf{q}$ are uniquely determined up to a scalar. This means, choosing random $\mathbf{p} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}$, $\mathbf{q} \in \mathbb{F}_q^l \setminus \{\mathbf{0}\}$ uniformly, and setting $\mathbf{u} = \mathbf{p}\mathbf{q}^T$, gives a random matrix of rank 1 with uniform distribution.

Actually we will use a slightly different model. Let

$$X_{k\times l} = \{\mathbf{u} \in \mathbb{F}_q^{k\times l};\ \mathrm{rk}\,\mathbf{u} \leq 1\}$$

be the set of rank 1 matrices together with the zero matrix. Pick random $\mathbf{p} \in \mathbb{F}_q^k$, $\mathbf{q} \in \mathbb{F}_q^l$ uniformly (possibly zero), and set $\mathbf{u} = \mathbf{p}\mathbf{q}^T$. This gives our distribution $\mathscr{L}$ on $X_{k\times l}$.

Note that if $\mathbf{u} \in X_{k\times l}$ is distributed according to $\mathscr{L}$, then conditioning on the event $\mathbf{u} \neq \mathbf{0}$ gives back the uniform distribution on matrices of rank 1. Conversely, if b is a Bernoulli variable of parameter $\mathbb{P}[b = 1] = (1-q^{-k})(1-q^{-l})$, and if $\mathbf{u}$ is a random uniformly distributed matrix of rank 1, then $b\mathbf{u} \in X_{k\times l}$ is distributed according to $\mathscr{L}$. Moreover, replacing $\mathbf{u_1}, \ldots, \mathbf{u_n}$ with $b_1\mathbf{u_1}, \ldots, b_n\mathbf{u_n}$ can only decrease the dimension of their linear span. As a consequence, any upper bound on $\mathbb{P}(n)$ for $(X_{k\times l}, \mathscr{L})$ will also be an upper bound for uniformly distributed matrices of rank 1.

Lemma 12. *(i) Every linear form on $\mathbb{F}_q^{k\times l}$ is of the form $l_{\mathbf{B}} = \mathrm{Tr}(\mathbf{B}^T\cdot)$ for a uniquely determined $\mathbf{B} \in \mathbb{F}_q^{k\times l}$.*

(ii) The number of $\mathbf{B} \in \mathbb{F}_q^{k\times l}$ of rank r is

$$\begin{bmatrix} k \\ r \end{bmatrix}_q \begin{bmatrix} l \\ r \end{bmatrix}_q |\mathrm{GL}_r(\mathbb{F}_q)| \leq C_q q^{r(k+l-r)}.$$

(iii) Given $\mathbf{B} \in \mathbb{F}_q^{k\times l}$ of rank r, then for random $\mathbf{u} = \mathbf{p}\mathbf{q}^T$ in $X_{k\times l}$ we have $\mathbb{P}[l_{\mathbf{B}}(\mathbf{u}) = 0] = \frac{1}{q}\left(1 + \frac{q-1}{q^r}\right)$.

Proof. Point (i) is clear. For point (ii) we view $\mathbf{B}$ as a linear map $\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^l$, and we note that it is entirely determined by its kernel $\ker\mathbf{B} \subseteq \mathbb{F}_q^k$ of codimension r, its image $\mathrm{im}\,\mathbf{B} \subseteq \mathbb{F}_q^l$ of dimension r, and the isomorphism $\mathbb{F}_q^k/\ker\mathbf{B} \simeq \mathrm{im}\,\mathbf{B}$

it induces. This gives the formula of the LHS, and the upper bound works as in the proof of Lemma 7. For (iii) we note $l_{\mathbf{B}}(\mathbf{u}) = 0$ means $\mathbf{p}^T\mathbf{B}\mathbf{q} = 0$, which happens precisely when $\mathbf{p}^T\mathbf{B} = 0$ (of probability q^{-r}) or when $\mathbf{q}$ is orthogonal to $\mathbf{p}^T\mathbf{B} \neq 0$ (of probability $q^{-1}(1-q^{-r})$). □

For some of our results we will restrict to matrices whose long side grows at most exponentially in the short side. More precisely, for any $\varepsilon, \kappa > 0$, we introduce the parameter space

$$\mathcal{P}(\varepsilon,\kappa) = \left\{(k,l);\ 2 \leq k \leq l \leq \frac{\varepsilon q^{\kappa k}}{(q-1)k}\right\}.$$

Now we fix a $\kappa > 0$ small enough so that $q^{(1-\kappa)^2} \geq 1 + \frac{q-1}{q}$ (for instance $\kappa = 0.23$ works for any q), as well as some $0 < \varepsilon < 1$.

Theorem 13. *Let $(k,l) \in \mathcal{P}(\varepsilon,\kappa)$ and $n \geq kl$. Then for random $\mathbf{u_1}, \ldots, \mathbf{u_n} \in X_{k\times l}$ we have*

$$\mathbb{P}[\mathbf{u_1}, \ldots, \mathbf{u_n} \text{ don't span } \mathbb{F}_q^{k\times l}] \leq c''\rho^{n-kl}$$

with $\rho = \frac{1}{q}\left(1 + \frac{q-1}{q}\right)$ and $c'' = \frac{qC_q}{(q-1)^2}\left(1 + \frac{1}{1-\varepsilon}\right)$.

Proof. We apply Corollary 5, where from Lemma 12 we get $\rho = \frac{1}{q}\left(1 + \frac{q-1}{q}\right)$ and

$$\begin{aligned} c' &\leq \frac{1}{q-1}\sum_{1\leq r\leq k} C_q q^{r(k+l-r)}\left(\tfrac{1}{q}\left(1+\tfrac{q-1}{q^r}\right)\right)^{kl} \\ &= \frac{C_q}{q-1}\sum_{1\leq r\leq k}\tfrac{\left(1+\frac{q-1}{q^r}\right)^{kl}}{q^{(k-r)(l-r)}}. \end{aligned}$$

We set $r_0 = \lfloor \kappa k \rfloor$ and split this last sum in two.

First, for $r \leq r_0$ we have $(k-r)(l-r) \geq (1-\kappa)^2 kl + (r_0 - r)$ and $1 + \frac{q-1}{q^r} \leq 1 + \frac{q-1}{q}$, so, by our condition on κ, $\frac{\left(1+\frac{q-1}{q^r}\right)^{kl}}{q^{(k-r)(l-r)}} \leq \frac{1}{q^{r_0-r}}$.

On the other hand, for $r > r_0$ we have $\left(1 + \frac{q-1}{q^r}\right)^{kl} < \left(1 + \frac{q-1}{q^{\kappa k}}\right)^{kl} \leq \frac{1}{1-\frac{kl(q-1)}{q^{\kappa k}}} \leq \frac{1}{1-\varepsilon}$.

We deduce:

$$c' < \frac{C_q}{q-1}\left(\sum_{1\leq r\leq r_0}\frac{1}{q^{r_0-r}} + \frac{1}{1-\varepsilon}\sum_{r_0<r\leq k}\frac{1}{q^{(k-r)(l-r)}}\right) \leq c''.$$

□

Given $k \leq l$ and random $\mathbf{u_i} \in X_{k\times l}$, recall for all $w \geq 1$ we set $\mathbf{s_w} = \mathbf{u_1} + \cdots + \mathbf{u_w} \in \mathbb{F}_q^{k\times l}$.

Theorem 14. *(i) For $1 \le w < k+l$ we have*

$$\mathbb{P}[\mathbf{s_w} = 0] \le \frac{2qC_q/(q-1)}{q^{kw/2}}.$$

(ii) For $w \ge k+l$ we have

$$\mathbb{P}[\mathbf{s_w} = 0] \le \frac{C_q(1-q^{-(w-l)})^{-1}}{q^{kl}}.$$

Proof. Write $\mathbf{u_i} = \mathbf{p}_i \mathbf{q_i}^T$ with $\mathbf{p_i} \in \mathbb{F}_q^k$, $\mathbf{q_i} \in \mathbb{F}_q^l$ uniform. Let G be the $k \times w$ matrix whose columns are $\mathbf{p_1}, \ldots, \mathbf{p_w}$, and let $\mathbf{x_1}, \ldots, \mathbf{x_k} \in \mathbb{F}_q^w$ be its rows. Likewise let G' be the $l \times w$ matrix whose columns are $\mathbf{q_1}, \ldots, \mathbf{q_w}$, and let $\mathbf{y_1}, \ldots, \mathbf{y_l} \in \mathbb{F}_q^w$ be its rows. Note these $\mathbf{x}$'s and $\mathbf{y}$'s are uniform and independent. Also our key observation is that $\mathbf{s_w} = 0$ iff $\langle \mathbf{x_1}, \ldots, \mathbf{x_k} \rangle \perp \langle \mathbf{y_1}, \ldots, \mathbf{y_l} \rangle$ in $\mathbb{F}_q^w$.

Now we condition on $\dim\langle \mathbf{y_1}, \ldots, \mathbf{y_l} \rangle$.

By Proposition 8 we have $\mathbb{P}[\dim\langle \mathbf{y_1}, \ldots, \mathbf{y_l} \rangle = e] \le C_q q^{-(l-e)(w-e)}$. Also, $\mathbb{P}[\langle \mathbf{x_1}, \ldots, \mathbf{x_k} \rangle \perp \langle \mathbf{y_1}, \ldots, \mathbf{y_l} \rangle \,|\, \dim\langle \mathbf{y_1}, \ldots, \mathbf{y_l} \rangle = e] = q^{-ke}$. This gives

$$\mathbb{P}[\mathbf{s_w} = 0] \le C_q \sum_{0 \le e \le \min(l,w)} q^{-f(e)}$$

where $f(e) = ke + (l-e)(w-e)$. This function f attains its minimum at $e_0 = (l+w-k)/2$, from which we deduce, for $0 \le e \le \min(l,w)$:

$$f(e) \ge \begin{cases} kw + (w-e) \ge kw/2 + (w-e) & \text{for } w \le l-k \\ f(e_0) + \lfloor |e-e_0| \rfloor \ge kw/2 + \lfloor |e-e_0| \rfloor & \text{for } l-k < w < k+l \\ kl + (e-k)(w-l) & \text{for } w \ge k+l. \end{cases}$$

The first two cases together give point (i), while the third gives point (ii). □

Theorem 15. *Let $(k,l) \in \mathcal{P}(\varepsilon, \frac{1}{2})$ and $n \le kl$. Then for random $\mathbf{u_1}, \ldots, \mathbf{u_n} \in X_{k\times l}$ we have*

$$\mathbb{P}[\mathbf{u_1}, \ldots, \mathbf{u_n} \textit{ lin. dependent}] \le \frac{qC_q}{(q-1)^2}\left(\frac{2\varepsilon}{1-\varepsilon} + q^{-(kl-n)}\right).$$

Proof. Split the sum in Proposition 10 in two: for $w < k+l$ use Theorem 14(i) and $\binom{n}{w} \le (kl)^w$; for $w \ge k+l$ use Theorem 14(ii). □

4 Products of codes

By a generating matrix for a linear code C we mean any matrix G whose row span is C. We allow G to have more than $\dim C$ rows.

Consider random $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, $\mathbf{G'} \in \mathbb{F}_q^{l\times n}$ (uniform distribution), generating matrices for $C, C' \subseteq \mathbb{F}_q^n$, so $\dim C \le k$, $\dim C' \le l$. Denote by $\mathbf{p_1}, \ldots, \mathbf{p_n} \in \mathbb{F}_q^k$

the columns and by $\mathbf{x_1}, \ldots, \mathbf{x_k} \in \mathbb{F}_q^n$ the rows of G. Denote by $\mathbf{q_1}, \ldots, \mathbf{q_n} \in \mathbb{F}_q^l$ the columns and by $\mathbf{y_1}, \ldots, \mathbf{y_l} \in \mathbb{F}_q^n$ the rows of G'.

Identify the matrix space $\mathbb{F}_q^{k\times l}$ with $\mathbb{F}_q^{kl}$.

The product $C * C'$ and its generating matrix $\widehat{G} \in \mathbb{F}_q^{(k\times l)\times n}$ admit the following equivalent descriptions [9]:

(i) $\widehat{G}$ has rows all products $\mathbf{x_i} * \mathbf{y_j}$

(ii) $C * C'$ is the projection of $C \otimes C'$ on the diagonal

(iii) $\widehat{G}$ has columns the rk ≤ 1 matrices $\mathbf{p_1}\mathbf{q_1}^T, \ldots, \mathbf{p_n}\mathbf{q_n}^T$

(iv) $C * C'$ is the image of the evaluation map

$$\begin{array}{rccc} \text{ev}\colon & \text{Bilin}(\mathbb{F}_q^k \times \mathbb{F}_q^l) & \longrightarrow & \mathbb{F}_q^n \\ & B & \mapsto & (B(\mathbf{p_1},\mathbf{q_1}), \ldots, B(\mathbf{p_n},\mathbf{q_n})). \end{array}$$

From description (iii) we can translate our Theorems 13 and 15. Recall $q^{(1-\kappa)^2} \geq 1 + \frac{q-1}{q}$, and $0 < \varepsilon < 1$.

Theorem 16. *For $(k,l) \in \mathcal{P}(\varepsilon, \kappa)$ and $n \geq kl$, we have*

$$\mathbb{P}[\dim C * C' < kl] \leq c'' \rho^{n-kl}$$

with $\rho = \frac{1}{q}\left(1 + \frac{q-1}{q}\right)$ and $c'' = \frac{qC_q}{(q-1)^2}\left(1 + \frac{1}{1-\varepsilon}\right)$.

Theorem 17. *For $(k,l) \in \mathcal{P}(\varepsilon, \frac{1}{2})$ and $n \leq kl$, we have*

$$\mathbb{P}[\dim C * C' < n] \leq \frac{qC_q}{(q-1)^2}\left(\frac{2\varepsilon}{1-\varepsilon} + q^{-(kl-n)}\right).$$

Note that if $k \to \infty$ and $kl/q^{k/2} \to 0$ (for instance if l is polynomial in k), we can set $\varepsilon = (q-1)kl/q^{k/2} \to 0$.

Still, we can derive an unconditional result, valid for any (k,l). Recall the maximum distance $\mathrm{d_{max}}$ of a linear code is the *maximum* weight of a codeword.

Theorem 18. *For any (k,l), and $k + l \leq n \leq kl$, we have*

$$\mathbb{P}[\mathrm{d_{max}}(C * C')^\perp \geq k + l] \leq \frac{qC_q}{(q-1)^2} q^{-(kl-n)}.$$

Proof. Union bound for $\mathbb{P}[\exists$lin. rel. of weight $\geq k + l]$, which means keep only terms $w \geq k + l$ in Proposition 10, and use only part (ii) of Theorem 14. □

So, with high probability $(C * C')^\perp$ has $\mathrm{d_{max}} < k + l$. This is a strong restriction (for instance it also implies $\dim < k + l$).

5 Squares and higher powers

Let C have generating matrix $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, with columns $\mathbf{p_1}, \ldots, \mathbf{p_n} \in \mathbb{F}_q^k$ and rows $\mathbf{x_1}, \ldots, \mathbf{x_k} \in \mathbb{F}_q^n$. As above, the s-th power $C^{\langle s\rangle}$ and its generating matrix $\widehat{G}$ admit the following equivalent descriptions:

(i) $\widehat{G}$ has rows all $*$-monomials of degree s in the $\mathbf{x_i}$

(ii) $C^{\langle s\rangle}$ is the projection of $C^{\otimes s}$ on the diagonal

(iii) $\widehat{G}$ has columns the elementary tensors $\mathbf{p_1}^{\otimes s}, \ldots, \mathbf{p_n}^{\otimes s}$

(iv) $C^{\langle s\rangle}$ is the image of the evaluation map

$$\begin{array}{rccc} \mathrm{ev}\colon & \mathbb{F}_q[t_1,\ldots,t_k]_s & \longrightarrow & \mathbb{F}_q^n \\ & P & \mapsto & (P(\mathbf{p_1}),\ldots,P(\mathbf{p_n})). \end{array}$$

(Where R_s denotes the s-th homogeneous component of R.)

We deduce at once $\dim C^{\langle s\rangle} \le \min(n, \binom{k+s-1}{s})$. For $s = 2$ it is shown in [4] that for random such C, with high probability there is equality: $\dim C^{\langle 2\rangle} = \min(n, \frac{k(k+1)}{2})$ (which could in turn be translated into a general position result for rank 1 symmetric matrices). It is interesting to note that not having to face unbalanced (k, l) made it easier for these authors to deal with short relations, hence to control $\mathrm{d}_{\min}(C^{\langle 2\rangle})^\perp$ in [4, Prop. 2.4]. By contrast, in our setting, independence of C and C' made it easier to deal with long relations, hence to control $\mathrm{d}_{\max}(C * C')^\perp$ in Theorem 18.

Concerning higher powers, one should be careful of the:

Proposition 19. *For $s > q$ we always have strict inequality*

$$\dim C^{\langle s\rangle} < \binom{k+s-1}{s}.$$

More precisely, we have

$$\dim C^{\langle s\rangle} \le \min(n, \chi_q(k, s))$$

where [9, App. A]:

$$\chi_q(k, s) = \dim S^s_{Frob}\mathbb{F}_q^k = \dim(\mathbb{F}_q[t_1,\ldots,t_k]/(t_i^q t_j - t_i t_j^q))_s.$$

Proof. The map $*$ is Frobenius-symmetric, so in (ii) the projection $C^{\otimes s} \to C^{\langle s\rangle}$ factors through $S^s_{\mathrm{Frob}}C$. Alternatively, in (iv), ker(ev) contains all multiples of the $t_i^q t_j - t_i t_j^q$. □

6 Open problems

In our probabilistic model we considered random matrices of the form $\mathbf{u_i} = \mathbf{p_i q_i}^T$ for column vectors $\mathbf{p_i} \in \mathbb{F}_q^k$, $\mathbf{q_i} \in \mathbb{F}_q^l$ possibly zero. However, as already

noted, it is perhaps more natural to restrict these $\mathbf{p_i}, \mathbf{q_i}$ to stay nonzero, so the $\mathbf{u_i}$ become uniformly distributed rank 1 matrices. Considering the $\mathbf{p_i}$ (resp. $\mathbf{q_i}$) as the columns of a generating matrix of a code C (resp. C'), this translates into considering only codes with full support—although of dimension possibly less than k (resp. l). Then, a further model would be to request these generating matrices having full rank. That means: take C (resp. C') uniformly distributed in the set of $[n,k]$ (resp. $[n,l]$) codes with full support. Clearly this could only help get sharper bounds. In particular:

Problem 20. *Do these alternative models allow to relax our condition $\mathcal{P}(\varepsilon,\kappa)$? Do they give bounds valid without any restriction on (k,l)?*

Proposition 11 suggests that the fate of long relations should essentially not depend on the probabilistic model. On the other hand, for short relations, it certainly does. In fact, relations of weight less than $k+l$ are perhaps less tractable because, for such a length, C and C' necessarily intersect. This leads to the following, which would encompass both our results (remove the conditioning) and those of [4] (set $i=k=l$):

Problem 21. *For any n,k,l,i,j, estimate the conditional probability*

$$\mathbb{P}[\dim C * C' = j \,|\, \dim C \cap C' = i].$$

We saw the existence of relations of length w is related to the distribution of $\mathbf{s_w} = \mathbf{u_1} + \cdots + \mathbf{u_w}$. When the $\mathbf{u_i}$ are uniformly distributed matrices of rank 1, this reduces to:

Problem 22. *In $\mathbb{F}_q^{k\times l}$, what is the number*

$$N_q^{k\times l}(r,w)$$

of decompositions of a matrix of rank r as an ordered sum of w matrices of rank 1?

It is easily seen that this number is well defined, which means, it is the same for all such matrices of rank r. Of special importance are the $N_q^{k\times l}(0,w)$, which control $\mathbb{P}[\mathbf{s_w}=0]$. We leave it as an exercise to link their computation with that of the weight distribution of the code $(S_k \otimes S_l)^\perp$, where S_k is the $[\frac{q^k-1}{q-1},k]$ q-ary simplex code.

Considering powers of a code leads similarly to count families of elementary s-th power tensors summing to zero.

Problem 23. *For fixed s, and a random $[n,k]$ code C, estimate the probability* $\mathbb{P}[\dim C^{\langle s\rangle} = \min(n, \chi_q(k,s))]$.

And then, what if we also let s vary?

It is interesting to note that, up to code equivalence, any $[n,k]$ code C with full support can be obtained from the simplex code S_k by deleting and repeating columns. Then $C^{\langle s\rangle}$ is obtained from $S_k^{\langle s\rangle}$ by deleting and repeating the same

columns. Some authors also call $S_k^{\langle s \rangle}$ the s-th order projective Reed-Muller code (in k variables); it has dimension $\chi_q(k,s)$. As above, we can split our Problem in two cases: for $n \geq \chi_q(k,s)$, we're interested in relations between rows of the generating matrix of C, which is linked to the weight distribution of $S_k^{\langle s \rangle}$; while for $n \leq \chi_q(k,s)$, we're interested in relations between columns, which is linked to its dual weight distribution.

Last, it is the author's opinion that considering only the dimension of products is not entirely in the spirit of coding theory. In fact, it is a purely algebraic problem, where $(\mathbb{F}_q^n, *)$ could be replaced by any space equipped with a bilinear inner composition law. See [1] for an example where the space is an extension field with its natural multiplication. However, what is genuinely coding-theoretic is to consider minimum distance beside dimension. It is well known that, asymptotically, a random code lies on the Gilbert-Varshamov bound $R = 1 - H(\delta)$. It is then very natural to ask:

Problem 24. *Does the product of two random codes, or the square or higher powers of a random code, lie on the GV bound?*

Observe that the answer would be negative if the question were stated with tensor product instead of $*$-product.

References

[1] C. Bachoc, O. Serra, and G. Zémor. "An analogue of Vosper's theorem for extension fields". Preprint, available: `http://arxiv.org/abs/1501.00602`

[2] R. Barbulescu, J. Detrey, N. Estibals, and P. Zimmermann. "Finding optimal formulae for bilinear maps", in *Arithmetic of Finite Fields — WAIFI 2012* (Lecture Notes in Comp. Science, vol. 7369), F. Özbudak and F. Rodriguez-Henriquez, Eds. Berlin: Springer-Verlag, 2012, pp. 168-186.

[3] R. W. Brocket and D. Dobkin, "On the optimal evaluation of a set of bilinear forms", *Lin. Alg. Appl.*, vol. 19, pp. 624-628, 1978.

[4] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor, "Squares of random linear codes", *IEEE Trans. Inform. Theory*, vol. 61, 2015. To appear.

[5] A. Couvreur, P. Gaborit, V. Gauthier, A. Otmani, and J.-P. Tillich. "Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes", *Des. Codes Crypto.*, Vol. 73, pp. 641-666, 2014.

[6] A. Couvreur, A. Otmani, and J.-P. Tillich. "Polynomial time attack on wild McEliece over quadratic extensions", in *Advances in Cryptology — EUROCRYPT 2014* (Lecture Notes in Comp. Science, vol. 8441), Ph. Nguyen and E. Oswald, Eds. Berlin: Springer-Verlag, 2014, pp. 17-39.

[7] A. Lempel and S. Winograd, "A new approach to error-correcting codes", *IEEE Trans. Inform. Theory*, vol. 23, pp. 503-508, 1977.

[8] H. Randriambololona, "Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method", *J. Complexity*, vol. 28, pp. 489-517, 2012.

[9] H. Randriambololona, "On products and powers of linear codes under componentwise multiplication", in: *Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT-14)* (Contemporary Math., vol. 637). AMS, 2015. To appear.

[10] H. Whitney, "On the abstract properties of linear independence", Amer. J. Math., vol. 57, pp. 509-533, 1935.